A Brief Review of Face Anti-Spoofing Methods

Dr. Raghavendra R. J[1], Vanishree P[2], Sparsha P[3], Thanuja K.V[4], Rhutu Y[5]

[1]Department of Information Science and Engineering, JNN College of Engineering, Shimoga-577204, Karnataka, India

Abstract: *Face anti-spoofing (FAS) has attracted increasing attention due to its vital role in securing face recognition systems from presentation attacks (PAs). In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in face recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found. This path of technological progression has naturally led to a critical issue that has only started to be addressed recently. The spoofing term referred to presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a face identification system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the face to the sensor. The entire face biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient ant-spoofing methods against this threat. The goal of this paper is to provide a comprehensive survey on the work that has been carried out previously in the emerging field of face anti-spoofing. The paper covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the future of this very active field of research.*

Keywords: face anti-spoofing, Local Binary Pattern, Texture Analysis, Biometrics

INTRODUCTION

Face anti-spoofing (FAS) is a security measure designed to detect and prevent fraudulent attempts to deceive face recognition systems by using spoofed representations, such as photographs, videos, or masks, instead of a live human face. Face recognition systems are increasingly susceptible to spoofing attacks, where an individual attempts to deceive biometric systems by presenting a fake face. Research has demonstrated the vulnerabilities of these systems for instance, a study found that while only 39% of images from social networks could be used for

spoofing, this was sufficient to fool 77% of users across six commercial face authentication systems [1]. Additionally, a live demonstration at the International Conference on Biometrics (ICB 2013) showcased how a female intruder successfully bypassed a face recognition system using makeup [2]. Current research on face spoofing detection has primarily focused on Gray-scale images, often neglecting color information that could aid in distinguishing genuine faces from fakes [3].

Although methods based on Gray-scale analysis have shown, their generalization capabilities remain questionable [4]. The limitations of Gray-scale analysis are evident, as the human eye is more sensitive to luminance than chroma, making it difficult to identify textural differences between genuine and fake faces in low-resolution images. However, examining the chroma component reveals some distinguishing characteristics. To address these challenges, author propose a novel face anti-spoofing method that leverages color texture analysis. Utilizing the color Local Binary Patterns (LBP) descriptor [5]. This approach extracts joint color-texture information from face images across three color spaces: RGB, HSV, and YCbCr. Extensive experiments conducted on the CASIA face anti-spoofing and Replay-Attack databases demonstrate that our color texture-based method outperforms traditional gray-scale techniques in detecting spoofing attacks.

The gradient issue in face spoofing detection (FSD) is a significant concern, as it underscores the reliance on physical, physiological, and behavioural characteristics to thwart fraud in security systems that depend on information or tokens [6]. Effective FSD requires through pre-processing of images to enhance feature extraction, as inadequate noise reduction can adversely affect classification accuracy [7]. The periocular region of the face, known for its distinctiveness, presents a promising area for improving recognition rates. This region can be analyzed using both global and local descriptors, allowing for a more nuanced understanding of facial features [8]. A discriminative model that incorporates MLBP descriptors has been developed to extract features from normalized images, although the MLBP method has limitations that may lead to inaccuracies in FSD.

The FAS task emphasizes analysing the texture and structural details of the face, as well as the realism of the background illumination. Early FAS methods

relied on traditional feature descriptors, such as Scale-Invariant Feature Transform (SIFT) [9], and Histogram of Oriented Gradients (HOG) [10]. However, recent advancements have shifted towards deep learning approaches, particularly convolutional neural networks (CNNs), which leverage multiple convolutional layers to enhance feature representation. To further refine the extraction of fine-grained information, some studies have introduced pixel-level supervision frameworks, enhancing the model's ability to capture detailed features. The proposed convolutional approach in this paper emphasizes shallow texture information and incorporates a multi-scale fusion module to effectively combine shallow style and deep structural information, thereby improving texture feature extraction capabilities. Furthermore, Raghavenda et al., [27-38] suggested many face anti-spoofing descriptors using texture-based method.

Experimental results indicate that this method outperforms previous models, such as Auxiliary [11] and CDCN [12], demonstrating strong performance in FAS tasks. In typical applications, the system processes video input, analysing sequences of frames to identify facial regions and key features, such as the corners of the head, eyes, and lips, to detect potential spoofing [13]. Additionally, corner points are detected using Shitomasi and FAST corner detection methods, enhancing the system's ability to identify spoofed faces effectively. Despite their widespread use and improvements in accuracy and reliability, these systems are still susceptible to various spoofing attacks, including simple photograph-based attempts and more sophisticated 3D mask attacks [14]. Consequently, developing effective anti-spoofing measures is crucial for protecting these systems against unauthorized access.

These models provide high efficiency and robust performance, making them suitable for real-time processing on devices with limited computational resources. This paper focuses on MobileNetV3, a model known for its exceptional balance between accuracy and efficiency, which has been previously adapted for physical FAS and is referred to as "MobileNetV3-Spoof" in this study. The periocular region of the face, which is less affected by gradient issues, offers significant potential for improving recognition rates due to its unique characteristics. This area is ideal for making a strong first impression and can be analysed using both global and local

descriptors [15]. Spatial information about faces is essential for tasks such as face identification and recognition. Despite its effectiveness, FSD faces challenges such as variations in lighting and head angles, which can complicate recognition efforts. To enhance accuracy, FSD can be combined with other biometric traits, such as fingerprints and palm veins.

The innovative use of dynamic kernels inspired by IADG and style transfer AdalN inspired by SSAN [16]. These methodologies work in tandem to facilitate the extraction of domain-invariant features. There is an efficient network structure that applies distinct normalization techniques to facial and texture features separately, allowing for the targeted minimization of domain-specific characteristics that could hinder model performance on novel datasets. Additionally, our model incorporates a modified version of supervised contrastive loss and smooth L1 loss to enhance the learning process. The supervised contrastive loss emphasizes texture features indicative of spoofing attempts, while the smooth L1 loss reduces the influence of content features, thereby improving the model's overall robustness and adaptability.

Numerous face liveness detection techniques have been developed to protect recognition systems from such attacks, demonstrating good performance on existing face presentation attack databases. Nonetheless, their effectiveness often deteriorates under real-world conditions, such as variations in illumination and camera quality. The demand for reliable identification and authentication methods is increasingly pressing, particularly with the proliferation of smartphones equipped with advanced front-facing cameras and enhanced computational power. Major platforms like Apple and Android have integrated face recognition systems into their operating systems, allowing users to unlock their devices securely. Among the many face liveness detection techniques, two primary categories have emerged: facial motion detection and facial texture analysis.

Motion detection methods require subjects to perform specific facial gestures, while texture analysis techniques focus on the high-frequency details in facial images, which can help distinguish between real and fake faces. Multi-scale filtering techniques are also employed to mitigate the effects of noise and illumination variations. Recent years have seen a surge in research focused on face

forgery detection. Early methods [17] primarily relied on handcrafted features and physiological signals to identify forgery traces. More recent approaches have employed convolutional neural networks (CNNs) to learn semantic features in an end-to-end manner. While these techniques have shown promising results when training and testing data are derived from the same dataset, they often experience significant performance drops in real-world scenarios characterized by diverse forgery methods and post-processing operations.

Consequently, enhancing robustness has become a critical concern in deep forgery detection. To tackle this challenge, many researchers have explored the frequency domain [19], finding that frequency domain features can effectively address detection issues related to compression. However, reliance on frequency domain features can lead to a marked decrease in generalization performance, as different datasets may involve various post-processing operations, making these methods vulnerable to specific adaptations as a result, many frequencies domain-based detection techniques exhibit serious limitations in practical applications a dual-stream detection architecture that leverages both texture and RGB features. By utilizing global texture information, the model reveals blending boundaries created by face-changing technologies, while local texture features expose subtle artifacts from attribute manipulation techniques.

To effectively harness texture information across different scales, author propose a feature pyramid module. With the rise of deep learning, deep networks have been integrated into FAS detection [20]. However, these binary classification models are often prone to overfitting, prompting researchers to employ auxiliary supervision methods, such as depth maps to enhance generalization performance. Recent advancements in vision transformers (ViT) have also been applied to FAS, yielding promising results [21]. Notably, the face anti-spoofing with language-image pretraining (FLIP) utilized the contrastive language-image pretraining (CLIP) model [22] for the first time, achieving excellent performance. In contrast to FLIP, our approach emphasizes the extraction of fine-grained features that remain invariant across different environments, particularly focusing on local features within images, such as edges in print attacks.

Here author conceptualize the binary classification problem of FAS as a pairwise similarity learning (PSL) problem. Existing proxy-based PSL methods [23] have demonstrated benefits for convergence and training stability; however, they require the design of additional loss functions to enforce specific similarity standards, complicating the training process to address these challenges, author propose improvements to FLIP. Our goal is to learn a generalized feature space in the source domain by cropping patches of a certain size from original face images to capture spoof-specific features. Inspired by previous work [24], author implement a patch loss to regularize the patch embedding space. Additionally, author introduce a dynamic central difference convolutional (DCDC) adapter for the image encoder to enhance the extraction of spoof features. Motion-based methods detect counterfeit faces by measuring eye and head movements, eye blinking, and changes in facial expressions [25].

While these methods are simple and fast, they primarily rely on eye movement, making them ineffective against sophisticated spoofing attacks that accurately mimic eye behaviour. Conversely, texture-based methods leverage lighting characteristics that differ between 2D and 3D objects or analyse fine texture differences between live and spoofed faces through external mediums like prints [26]. These methods often utilize local image descriptors to capture texture differences. Although texture-based methods are favoured for their ease of implementation and quick detection times, they struggle with classifying liveness in non-uniform images or those with significant noise. Our method analyses combined color-texture information in terms of luminance and color difference channels, employing LBP descriptors. Specifically, author utilize the Cb, S, and H bands from the color spaces for this analysis. the advancements in face recognition and anti-spoofing technologies have significantly enhanced security in various applications, from mobile devices to banking transactions. However, challenges remain due to vulnerabilities to spoofing attacks and the limitations of existing detection methods, particularly in cross-domain scenarios

Review Methodology:

The methodology for face anti-spoofing detection begins with input acquisition, where a face video is captured containing both real and spoofing face

images. The process then moves to preprocessing, which involves detecting faces within the video and cropping the detected face region. The cropped face image is normalized to a fixed size of pixels to ensure consistency for further processing. Following preprocessing, the normalized face image is converted into the YCbCr color space, separating brightness from color information. Feature extraction is performed using three descriptors: Co-occurrence of Adjacent Local Binary Patterns (CoALBP), which captures rich texture and spatial structure information; Local Phase Quantization (LPQ), which enhances image quality by addressing blur insensitivity and improving resolution; and Local Directional Number Pattern from Three Orthogonal Planes (LDN-TOP), which encodes structural information and brightness intensity changes, providing robust features against lighting variations.

The features extracted from these descriptors are combined to form a comprehensive feature histogram representing the face image. Finally, this combined feature histogram is fed into a binary classifier, such as a Support Vector Machine (SVM), to determine whether the face in the input image is real or a spoofing attempt, resulting in a decision that indicates the authenticity of the face image. This methodology effectively integrates multiple descriptors enhance the accuracy of face anti-spoofing detection, leveraging both color texture and brightness information to improve classification performance. The methodology for Deep learning based intelligent system for robust face spoofing detection using texture feature measurement using NLBP-Net involves a systematic approach to detect and classify face images as real or spoofed.

The process begins with input acquisition, where face images are captured and fed into the system. The next step is preprocessing, which involves detecting the face within the image and cropping the face region to focus on the relevant features. This is crucial for removing any unnecessary background information and ensuring that the subsequent processing steps are effective. The cropped face image is then normalized to a standard size to ensure consistency. Following preprocessing, the face image proceeds to the feature extraction phase, where Local Binary Pattern (LBP) is used to extract features from the image. LBP is particularly effective in capturing the unique characteristics of the face, including the periocular area, which remains untouched by the gradient process and is highly unique. The

extracted features are then trained using the advanced Visual Geometry Group 16 (VGG16) methods, which enables the model to learn complex patterns and relationships in the data.

The trained model is then used to classify the face image as real or spoofed. This is achieved through a deep learning Convolutional Neural Network (DLCNN) architecture, which is designed to effectively classify spoofing and faking attempts in random face images. The classifier takes the extracted features as input and outputs a decision indicating whether the face image is real or spoofed. The methodology for A Single-frame face anti-spoofing algorithm with circular CDC and Multi-Scale Spatial Attention involves a multi-step approach to prevent face images with attack properties from entering face recognition systems. The process begins with input acquisition, where face images are captured and fed into the system. The next step is preprocessing, which involves detecting the face within the image and cropping the face region to focus on the relevant features.

This is crucial for removing any unnecessary background information and ensuring that the subsequent processing steps are effective. Following preprocessing, the face image proceeds to the feature extraction phase, where a circular Central Difference Convolution (CDC) is used to extract texture features and multi-scale information. The CDC is designed with a larger sensory field and contextual semantic awareness, allowing it to capture more detailed information from the face image. The extracted features are then combined with spatial attention method, which concatenates multiple scale feature maps to fuse the feature map information from multiple scales. The feature maps are then fed into a backbone network, which is designed to improve the network model's ability to characterize texture features and multi-scale information. The network is trained to detect face spoofing attacks by learning the differences between real and fake face images. Finally, the output of the network is used to classify the face image as real or spoofed.

The methodology for An Enhanced Face Anti-Spoofing Model using Color Texture and Corner Feature based Liveness involves a multi-step approach to ensure the presence of a real human face in a photograph or 2D masks. The process begins with input acquisition, where a video is captured and fed into the system. The next

step is preprocessing, which involves extracting frames from the video and cropping the face region to focus on the specific facial landmark points. Following preprocessing, the face image proceeds to the feature extraction phase, where the texture of the 2D masks and real face is analyzed by changing its colorspace. This is done to differentiate between the real face and fake face, as the texture of the 2D masks is different from that of the real face. The colorspace conversion is used to enhance the texture features of the face image. The next step is to detect the corner points of the face image using various corner detection algorithms.

The corner points are used to differentiate between the real face and fake face, as the corner points of the real face are more pronounced than those of the fake face. A threshold value is used to determine whether the face is real or fake based on the corner points. Finally, the feature maps are fed into a classifier, which is trained to detect face spoofing attacks by learning the differences between real and fake face images. The methodology for A Robust and Real-Time Face Anti-spoofing Method Based on Texture Feature Analysis involves a multi-step approach to classify faces as real or spoofed. The process begins with input acquisition, where a face image is captured and fed into the system. The next step is preprocessing, which involves detecting the face within the image and cropping the face region to focus on the relevant features. Following preprocessing, the face image is converted into grayscale and YCbCr color spaces to extract multiple texture features based on Local Binary Patterns (LBP). The LBP features are extracted from both the grayscale and YCbCr color spaces to capture a comprehensive representation of the face image.

The extracted LBP features are then used to train a binary Support Vector Machine (SVM) classifier, which is designed to classify faces as real or spoofed. The SVM classifier is trained on a dataset of real and spoofed face images to learn the differences between the two classes. Once the SVM classifier is trained, it is used to classify new face images as real or spoofed. The classifier outputs a decision indicating whether the face image is real or spoofed, based on the LBP features extracted from the image. The methodology for Assessing the Performance of Efficient Face Anti-Spoofing Detection Against Physical and Digital Presentation Attacks in this study focuses on the evaluation of pre-processing and training

methods using Lightweight Convolutional Neural Networks (CNNs), specifically MobileNetV3 with a spoofing detection head, referred to as "MobileNetV3-Spoof." The process begins with input acquisition, where face images are captured from the UniAttackData dataset, which encompasses a wide range of spoofing scenarios, including deepfake and adversarial attack samples.

The next step is preprocessing, which is critical for enhancing the model's performance. This involves detecting the face within the input images and cropping the face region to isolate the relevant features. The cropped face images are then subjected to alignment to ensure consistency in orientation and scale, which is essential for effective feature extraction. Once the features are extracted, they are fed into the spoofing detection head of the MobileNetV3-Spoof model. The classifier utilizes these features to determine whether the input face image is real or spoofed. The methodology for On the generalization of color texture-based face anti-spoofing in this study focuses on addressing the challenges of generalization in presentation attack detection (PAD) methods. The process begins with input acquisition, where face images are captured under various conditions, including different presentation attack instruments (PAIs) such as display and print attacks. Following preprocessing, the aligned face images are processed through a feature extraction phase that utilizes color texture analysis. This phase focuses on extracting color texture features from the face images, which are critical for distinguishing between real and spoofed faces. The extracted features are then represented in a way that captures the unique characteristics of the face, allowing for a more robust analysis against various PAIs. Once the features are extracted, they are fed into a classifier designed to detect whether the input face image is real or spoofed.

The methodology for Domain-Generalized Face Anti-Spoofing with Domain Adaptive Style Extraction in this study emphasizes domain generalization to enhance the robustness of face recognition systems across diverse environments. The process begins with input acquisition, where face images are captured from various sources, ensuring a wide range of scenarios and conditions are represented. Next, the methodology involves preprocessing, the aligned face images are processed through a feature extraction phase that prioritizes the distinction between textural and non-facial features. This approach allows the model to adapt to various

unseen domains without relying on domain-specific modifications. The model employs dynamic kernels and style transfer AdalN for domain-invariant feature extraction, which enhances its ability to mitigate vulnerabilities to environmental variations and different attack vectors. Once the features are extracted, they are fed into a classifier designed to perform binary classification between spoofed and live samples. This classifier simplifies the decision-making process, allowing for efficient detection of face spoofing attempts.

The methodology for the proposed Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods begins with input acquisition, where facial images are captured using a face detection camera. This initial step is crucial for gathering the necessary data for analysis. Following input acquisition, the methodology involves preprocessing, which is essential for preparing the images for further examination. This step includes detecting the cropped images are then processed using a modified Difference of Gaussian (DoG) filtering method. After preprocessing, the face images undergo feature extraction using the Local Binary Pattern Variance (LBPV) technique. This method is specifically designed to be invariant to rotation, allowing for consistent feature extraction regardless of the orientation of the face in the image. The extracted feature vectors are then prepared for classification.

Once the features are extracted, they are input into a Support Vector Machine (SVM) classifier. The SVM is trained to differentiate between real and spoofed faces based on the feature vectors derived from the images. The system is evaluated using the NUAA photo-imposter database, which contains facial images captured under various illumination conditions and angles. The methodology for the proposed facial forgery detection system begins with input acquisition, where facial images are captured for analysis. This initial step is crucial for ensuring that the system has access to the relevant data needed to identify potential forgeries. Following input acquisition, the methodology involves preprocessing, which is essential for preparing the images for further analysis. This step includes detecting the cropped images are then processed to enhance their quality and ensure consistency, which is vital for effective feature extraction.

After preprocessing, the face images are analysed using a two-stream detection architecture that integrates both texture features and RGB features. The system separately analyses global large texture information and local detailed texture information to capture subtle artifacts that may indicate forgery. Once the features are fused, they are input into a classifier designed to determine whether the face image is real or a forgery. The methodology for the proposed multimodal proxy-free face anti-spoofing (FAS) model begins with input acquisition, where facial images are captured for analysis. This initial step is crucial for ensuring that the system has access to the relevant data needed to identify potential spoofing attempts. Following input acquisition, the methodology involves preprocessing, which is essential for preparing the images for further analysis.

This step includes detecting the face within the captured images and cropping the face region to focus on local patches. After preprocessing, the cropped face patches are processed through a feature extraction phase that employs a Contrastive Language-Image Pre-training (CLIP) backbone. In addition to the feature extraction, a Dynamic Central Difference Convolutional (DCDC) adapter is introduced to enhance the extraction of detailed features from the patches Once the features are extracted, they are input into a classifier that utilizes a proxy-free pairwise similarity learning (PSL) loss function. This loss function is designed to ensure that the maximum intra-class distance is smaller than the minimum inter-class distance, thereby improving the model's ability to distinguish between real and spoofed faces. The methodology for the proposed Face anti spoofing method using color texture segmentation on FPGA begins with input acquisition, where facial images are captured for analysis.

This step is essential for ensuring that the system has access to the relevant biometric data needed for effective authentication. Following input acquisition, the methodology involves preprocessing, which is critical for preparing the images for further analysis. This step includes detecting the cropped face images are then processed to enhance their quality and ensure consistency, which is vital for effective feature extraction. After preprocessing, the cropped face images are analysed using a local binary pattern (LBP) descriptor to extract color-texture information. This analysis incorporates luminance and color difference channels,

specifically focusing on the Cb, S, and V bands within the color spaces. Once the features are extracted using the LBP descriptor, they are input into a convolutional neural network (CNN) classifier. The CNN is trained to differentiate between real and spoofed faces based on the extracted color-texture features.

Conclusions

In this survey paper, we have reviewed recent studies focused on face anti-spoofing (FAS) methods, highlighting the advancements and challenges in the field. The reviewed methods demonstrate a significant evolution in the detection of face spoofing attacks, leveraging various techniques such as convolutional neural networks (CNNs), local binary patterns (LBP), and dynamic color texture analysis to enhance accuracy and robustness. Key insights from the studies indicate that combining multiple feature extraction techniques such as color-texture information, local and global texture features, and brightness characteristics improves the detection capabilities of spoofing systems. The integration of advanced modules, including attention mechanisms and feature pyramids, has been shown to effectively capture subtle artifacts and enhance the overall detection performance.

Moreover, the importance of preprocessing steps, such as face detection and alignment, is emphasized as critical for improving model accuracy. The studies also highlight the necessity for models to generalize well across diverse datasets and real-world conditions, addressing the limitations of existing methods that often struggle with cross-database performance. While many proposed methods achieve state-of-the-art results on benchmark datasets, challenges remain in terms of computational efficiency and the ability to handle various spoofing techniques, such as printed photos and video replay attacks. Future research directions include optimizing models for real-time applications, exploring hybrid approaches, and enhancing the robustness of detection systems against emerging spoofing tactics. Overall, this survey underscores the ongoing need for innovative solutions in face anti-spoofing, with a focus on improving detection accuracy, generalization capabilities, and practical applicability in diverse environments. The insights gathered from these studies provide a foundation for future research aimed at advancing the field of biometric security.

References

[1] Yan Li, Ke Xu, Qiang Yan, Yingjiu Li, and Robert H. Deng, "Understanding osn-based facial disclosure against face authentication systems," in Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, New York, NY, USA, 2014, ASIA CCS'14, pp. 413–424, ACM.

[2] Tabula Rasa, "Tabula rasa spoofing challenge," Tech. Rep., 2013, http://www.tabularasa euproject.org/evaluations/tabula-rasa spoofingchallenge-2013.

[3] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in International Joint Conference on Biometrics (IJCB), Oct 2011, pp. 1–7.

[4] T. de Freitas Pereira, A. Anjos, J.M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real-world scenario," in International Conference on Biometrics (ICB), June 2013, pp. 1–8.

[5] Jae Young Choi, K.N. Plataniotis, and Yong Man Ro, "Using colour local binary pattern features for face recognition," in IEEE International Conference on Im age Processing (ICIP), Sept 2010, pp. 4541–4544.

[6] A.A. Nazarenko, G.A. Safdar, "Survey on security and privacy issues in cyber physical systems", AIMS Electron. Elect. Eng... 3 (2) (2019) 111–143.

[7] Abdullah Amer, Abdullah Yahya, Tamanna Siddique, "A novel algorithm for sarcasm detection using supervised machine learning approach", AIMS Electron. Elect. Eng. 6 (4) (2022) 345–369.

[8] Efe Francis Orumwense, Abo-Al-Ez Khaled, "Internet of Things for smart energy systems: a review on its applications, challenges and future trends", AIMS Electron. Elect. Eng. 7 (1) (2023) 50–74.

[9] K. Patel, H. Han, and A. K. Jain, "Secure face unlocks: Spoof detection on smartphones," IEEE Transactions on Information Forensics Security, vol. 11, no. 10, pp. 2268–2283, 2016.

[10] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing," in IEEE Sixth International Conference on Biometrics: Theory, 2014.

[11] Y. Liu, A. Jourabloo, and X. Liu, "Learning deep models for face anti-spoofing: Binary or auxiliary supervision," in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018.

[12] Z. Yu, C. Zhao, Z. Wang, Y. Qin, Z. Su, X. Li, F. Zhou, and G. Zhao, "Searching central difference convolutional networks for face anti spoofing," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 5294–5304.

[13] Nanthini N., Puviarasan N., Aruna P., An Efficient Velocity Estimation Approach for Face Liveness Detection using Sparse Optical Flow Technique, indian journal of science and technology., vol.14(25), pp.2128-2136, (2021).

[14] Ajian Liu, Chenxu Zhao, Zitong Yu, Anyang Su, Xing Liu, Zijian Kong, Jun Wan, Sergio Escalera, Hugo Jair Escalante, ZhenLei, et al. 3d high-fidelity mask face presentation attack detection challenge. In Proceedings of the IEEE/CVF Inter national Conference on Computer Vision Workshops, pages 814–823, 2021.

[15] Yoanna Martinez-Diaz, Miguel Nicolas-Diaz, Heydi Mendez-Vazquez, Luis S Luevano, Leonardo Chang, Miguel Gonzalez-Mendoza, and Luis Enrique Sucar. Bench marking lightweight face architectures on specific face recognition scenarios. Artificial Intelligence Review, pages 1–44, 2021.

[16] Efe Francis Orumwense, Abo-Al-Ez Khaled, Internet of Things for smart energy systems: a review on its applications, challenges and future trends, AIMS Electron. Elect. Eng. 7 (1) (2023) 50–74.

[17] Z. Wang, Z. Wang, Z. Yu, W. Deng, J. Li, T. Gao, and Z. Wang, "Domain generalization via shuffled style assembly for face anti-spoofing," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 4123–4133, 2022.

[18] Y.Z. Li, M.C. Chang, S.W. Lyu, "In exposing AI created fake videos by detecting eye blinking". In IEEE International Workshop on Information Forensics and Security (WIFS), 2018, pp. 1–7

[19] Y. Luo, Y. Zhang, J. Yan, and W. Liu, "Generalizing face forgery detection with high-frequency features". In CVPR, 2021, pp. 16317–16326

[20] Z. Li, J. Yuan, B. Jia, Y. He, and L. Xie, "An effective face anti spoofing method via stereo matching," IEEE Signal Process. Lett., vol. 28, pp. 847–851, 2021.

[21] K. Srivatsan, M. Naseer, and K. Nandakumar, "Flip: Cross-domain face anti-spoofing with language guidance," in Proc. IEEE/CVF Int. Conf. Comput. Vis., 2023, pp. 19685–19696.

[22] A. Radford et al., "Learning transferable visual models from natural language super vision," in Proc. Int. Conf. Mach. Learn., 2021, pp.8748–8763

[23] W.Liu, Y. Wen, Z. Yu, M. Li, B. Raj, and L. Song, "Sphereface: Deep hypersphere embedding for face recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2017, pp. 212–220

[24] C.-Y. Wang, Y.-D. Lu, S.-T. Yang, and S.-H. Lai, "Patchnet: A simple face anti-spoofing framework via fine-grained patch recognition," in Proc. IEEE /CVF Conf. Comput. Vis. Pattern Recognit., 2022, pp. 20281–20290.

[25] Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in Proceedings of the SPIE- International Society for Optics and Photonics, pp. 296–303, Choufu, Japan, March 2004.

[26] A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in Proceedings of the 2011 international joint conference on Biometrics (IJCB), pp. 1–7, IEEE, Washington, WA, USA, October 2011.

[27] Raghavendra, R. J., & Kunte, "DOG-ADTCP: A new feature descriptor for protection of face identification system", in Journal of Expert Systems with Applications, vol. 201, pp. 1-16, 2022.https://doi.org/10.1016/j.eswa.2022.117207

[28] Raghavendra R.J., Sanjeev Kunte R., "Extended Local Ternary Co-relation Pattern: a novel feature descriptor for face Anti-spoofing", in Journal of Information Security and Applications, vol. 52, pp. 1–10, 2020. https://doi.org/10.1016/j.jisa.2020.102482

[29] Raghavendra R.J., Sanjeev Kunte R., "Extended Local Ternary Pattern for Face Anti-spoofing", in proceedings of the Lecture Notes on Electrical Engineering, pp. 221–229, 2020. https://link.springer.com/chapter/10.1007/978-981-15-3125-5_24

[30] Raghavendra R.J., Sanjeev Kunte R., "Anisotropic Smoothing for Illumination Invariant Face Anti-spoofing", in proceedings of the International Conference on Trends in Electronics and Informatics IEEE, pp. 901–905, 2020. https://doi.org/10.1109/ICOEI48184.2020.9142948

[31] Raghavendra R.J., Sanjeev Kunte R., "A Novel Feature Descriptor for Face Anti- Spoofing using Texture Based Method", in proceedings of International Journal of Cybernetics and Information Technologies, vol. 20, pp. 159–176, 2020. https://doi.org/10.2478/cait-2020-0035

[32] Raghavendra R.J., Sanjeev Kunte R., "Face spoofing detection using machine learning approach", in International Journal of Innovative Research in Computer and Communication Engineering, vol. 7, pp. 21–26, 2019.https://doi.org/10.1016/j.cose.2023.103421

[33] Raghavendra R.J., Sanjeev Kunte R., "Extended right-angle difference ternary co-relation pattern: A new feature descriptor for face anti-spoofing", in International Journal of Computers and Security, vol. 134, pp. 1-14, 2023. https://doi.org/10.1016/j.cose.2023.103421

[34] Raghavendra R. J, Jeevan K. P, Likith M, Manoj G, Yashas D. S, "A Survey on Anti- Spoofing Methods for Facial Recognition", in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 8, 2022. https://doi.org/10.3390/jimaging6120139

[35] Raghavendra R.J., Priyanka S.S., Sampada H.K., Shamitha K.J., Khan S., "Face Biometric Antispoofing Methods: A Survey", in International Journal of Advanced Research in Computer and Communication Engineering, vol. 11, pp. 499–505, 2022. https://ijarcce.com/wp-content/uploads/2022/04/IJARCCE.2022.11387.pdf

[36] Raghavendra R.J., Srikanta Datta Kashyap A.P., Samarth B.N., Sathvik S.R., Shashikumara K., "A Reviews on Face Anti-Spoofing Methods", in International Journal of Creative Research Thoughts, vol. 11, pp. 331–338, 2023. https://ijcrt.org/papers/IJCRT2303256.pdf

[37] Raghavendra R.J., Jain D., Greeshma Lahari S.N., Bhumika K.R., Shariff S.A., "Countermeasures to Facial Spoofing Attacks: A Survey", in of Journal Gradiva Review, vol. 9, pp. 452–463, 2023.

[38] R. Raghavendra and R. Kunte, "A Novel Feature Descriptor for Face Anti-Spoofing Using Texture Based Method," Cybern. Inf. Technol., vol. 20, pp. 159–176, 2020.http://dx.doi.org/10.2478/cait-2020-0035